FORM PTO-1449

INFORMATION DISCLOSURE STATEMENT

ATTORNEY DOCKET NO.: RSA-052

APPLICANT: Kaliski, Jr.

SERIAL NO.: 09/802,485

FILING DATE: March 9, 2001

GROUP: 2131

U.S. PATENT DOCUMENTS

EXAM. INIT.		DOCUMENT NUMBER	DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE
pwk	A1	4,424,414	01/03/84	Hellman et al.	178	22.11	05/01/78
pwk	A2	4,567,600	01/28/86	Massey et al.	375	2.1	09/14/82
pwk	A3	4,720,860	01/19/88	Weiss	380	23	11/30/84
pwk	A4	4,759,063	07/19/88	Chaum	380	30	08/22/83
pwk	A5	4,885,778	12/05/89	Weiss	380	48	11/27/85
pwk	A6	4,947,430	08/07/90	Chaum	380	25	11/23/87
pwk	A7	5,023,908	06/11/91	Weiss	380	23	04/21/89
pwk	A8	5,168,520	12/01/92	Weiss	380	23	03/18/91
pwk	A9	5,222,140	06/22/93	Beller et al.	380	30	11/08/91
pwk	A10	5,241,599	08/31/93	Bellovin et al.	380	21	10/02/91
pwk	A11	5,367,572	11/22/94	Weiss	380	23	07/31/92
pwk	A12	5,440,635	08/08/95	Bellovin et al.	380	25	08/23/93
pwk	A13	5,485,519	01/16/96	Weiss	380	23	05/25/93
pwk	A14	6,240,184 B1	05/29/01	Huynh et al.	380	206	09/02/98

FOREIGN PATENT DOCUMENTS

EXAM. INIT.		DOCUMENT NUMBER	DATE	COUNTRY CODE	CLASS	SUB CLASS	FILING DATE	ABSTRACT ONLY	ENGLISH LANG (Y/N)

FORM PTO – 1449 **INFORMATION DISCLOSURE STATEMENT**	ATTORNEY DOCKET NO.: RSA-052 APPLICANT: Kaliski, Jr. SERIAL NO.: 09/802,485 FILING DATE: March 9, 2001 GROUP: 2131

OTHER ART, JOURNAL ARTICLES, ETC.

EXAM. INIT.	OTHER DOCUMENTS: (Including Author, Title, Date, Relevant Pages, Place of Publication)	
pwk	C1	Bellovin and Merritt, *"Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks"*, (pgs. 72-84); Proceedings of the IEEE Symposium on Research in Security and Privacy, May 1992
pwk	C2	Bellovin and Merritt, *"Augmented Encrypted Key Exchange: a Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise"*, (pgs. 1-7); AT&T Bell Laboratories Technical Report, 1994
pwk	C3	Boneh, DeMillo, and Lipton, *"On the Importance of Checking Cryptographic Protocols for Faults" (extended abstract)*, (pgs. 1-14); [online], [retrieved 2001-07-26], retrieved from the Internet URL:http://citeseer.nj.nec.com/boneh97importance.html
pwk	C4	Boneh and Franklin, *"Efficient Generation of Shared RSA Keys"*, (pgs. 1-21); [online], [retrieved 2001-07-26], retrieved from the Internet URL:http//citeseer.nj.nex.com/358268.html
pwk	C5	Cannetti and Gennaro, *"Proactive Security: Long-Term Protection Against Break-Ins"*, (pgs. 1-8); RSA Laboratories, CryptoBytes, Volume 3, Number 1, Spring 1997
pwk	C6	Chaum, *"Security Without Identification: Transaction Systems to Make Big Brother Obsolete,"* (pgs. 1030-1044); Communications of the ACM, October 1985, Volume 28 Number 10
pwk	C7	Chaum, *"Blind Signatures for Untraceable Payments"*, (pgs. 199-203); Advances in Cryptology, Proceedings of the Crypto '82, Workshop on the Theory and Application of Cryptographic Techniques, Santa Barbara, California, August 23-25, 1982, New York 1983
pwk	C8	Coron, Naccache, and Stern, *"On the Security of RSA Padding"*, (pgs. 1-18); Advances in Cryptology, Proceedings of the Crypto '99, Springer 1999
pwk	C9	Desmedt and Odlyzko, *"A Chosen Text Attack on the RSA Cryptosystem and Some Discrete Logarithm Schemes"*, (pgs. 516-522); Advances in Cryptology, Proceedings of Crypto '85, Springer-Verlag 1986
pwk	C10	Dierks and Allen, *"The TLS Protocol Version 1.0"*, (pgs. 1-75); IETF RFC 2246, January 1999, [online], [retrieved 2001-07-25], retrieved from the Internet URL:http://www.ietf.org/rfc/rfc2246.txt
pwk	C11	Frier, Karlton, and Kocher, *"The SSL 3.0 Protocol"*, (pgs. 1-62); Netscape Communications Corp., November 18, 1996, [online], [retrieved 2001-07-10], retrieved from the Internet URL:http://home.netscape.come/eng/ssl13/draft302.txt
pwk	C12	Gong, *"Increasing Availability and Security of an Authentication Service,"* (pgs. 657-662); IEEE Journal on Selected Areas in Communications, Volume 11, Number 5, June 1993
pwk	C13	Gong, Lomas, Needham, and Saltzer, *"Protecting Poorly Chosen Secrets From Guessing Attacks,"* (pgs. 648-656); IEEE Journal on Selected Areas in Communications, Volume 11, Number 5, June 1993
pwk	C14	Gong, *"Optimal Authentication Protocols Resistant to Password Guessing Attacks"*, (pgs. 24-29); Proceedings of the 8th IEEE Computer Security Foundations Workshop, Ireland, June 13-15, 1995
pwk	C15	Halevi and Krawczyk, *"Public-Key Cryptography and Password Protocols"*, (pgs. 122-131); Proceedings of the Fifth ACM Conference on Computer and Communications Security, November 3-5, 1998

FORM PTO – 1449 **SUPPLEMENTAL** **INFORMATION DISCLOSURE STATEMENT**	ATTORNEY DOCKET NO.: RSA-052 APPLICANT: Kaliski, Jr. SERIAL NO.: 09/802,485 FILING DATE: March 9, 2001 GROUP: 2131

pwk	C16	Heroux, *"A Private Key Storage Server for DCE – Functional Specification"*, (pgs. 1-73); Open Software Foundation, Request for Comments: 94.1, November 1996, [online], [retrieved on 2001-17-07], retrieved form the Internet URL:http://www.opengroup.org/rfc/mirror-rfc/rfc94.1.txt
pwk	C17	Herzberg, Jarecki, Krawczyk, and Yung, *"Proactive Secret Sharing Or: How to Cope With Perpetual Leakage"*, (pgs. 339-352); Advances in Cryptology, Proceedings of the Crypto '95, California, August 1995, Springer 1995
pwk	C18	Jablon, *"Strong Password-Only Authenticated Key Exchange"*, (pgs. 1-24); ACM Computer Communications Review, September 25, 1996
pwk	C19	Jablon, *"Extended Password Key Exchange Protocols Immune to Dictionary Attack"*, (pgs. 248-255); Proceedings of the WETICE '97 Enterprise Security Workshop, June 1997
pwk	C20	Juels, Luby, and Ostrovsky, *"Security of Blind Digital Signatures"*, (pgs. 150-164); Advances in Cryptology, Proceedings of the Crypto '97, California, August 1997, Springer 1997
pwk	C21	Kohl and Neuman, *"The Kerberos Network Authentication Service"*, (pgs. 1-105); RFC 1510, Internet Activities Board, September 1993, [online], [retrieved 2001-07-10], retrieved from the Internet URL:http://www.ietf.org/rfc/rfc1510.txt
pwk	C22	Law, Menezes, Qu, Solinas, and Vanstone, *"An Efficient Protocol for Authenticated Key Agreement"*, (pgs. 1-16); Technical Report CORR 98-05, Dept. of C&O, University of Waterloo, Canada, March 1998 (revised August 28, 1998)
pwk	C23	Lim and Lee, *"A Key Recovery Attack on Some Discrete Log-Based Schemes Using a Prime-Order Subgroup"*, (pgs. 249-263); Advances in Cryptology, Proceeding of the Crypto '97, Volume 1294 of Lecture Notes in Computer Science, Springer 1997
pwk	C24	Menezes, van Oorschot, and Vanstone, *"Handbook of Applied Cryptography"*, from Chapter 12 *Key Establishment Protocols*, Section 12.22 Protocol *Shamir's no-key protocol*, (pg. 500); CRC Press 1997
pwk	C25	M'Raihi, *"Cost-Effective Payment Schemes With Privacy Regulation"*, (pgs. 266-275); Advances in Cryptology, Proceedings of ASIACRYPT ' 96, Volume 1163 of LNCS, 1996
pwk	C26	MacKenzie and Swaminathan, *"Secure Network Authentication With Password Identification"*, (pgs. 1-11); Submission to IEEE P1363 a working group, July 30, 1999, [online], [retrieved 2001-07-10], retrieved form the Internet URL:http://www.manta.ieee.org/groups/;1363/studygroup/passwd.html
pwk	C27	Monrose, Reiter, and Wetzel, *"Password Hardening Based on Keystroke Dynamics"*, (pgs. 73-82); Proceedins of the 6th ACM Conference on Computer and Communications Security, November 1-4, 1999, Singapore, [online], [retrieved on 2000-09-06], retrieved from the Internet URL:http://www.acm.org/pubs/contents/proceedings/commsec/319709
pwk	C28	Perlman and Kaufman, *"Secure Password-Based Protocol for Downloading a Private Key"*, Proceedings of the 1999 Network and Distributed System Security Symposium, Internet Society, January 1999

FORM PTO – 1449 **INFORMATION DISCLOSURE STATEMENT**	ATTORNEY DOCKET NO.: RSA-052 APPLICANT: Kaliski, Jr. SERIAL NO.: 09/802,485 FILING DATE: March 9, 2001 GROUP: 2131

pwk	C29	Pohlig and Hellman, *"An Improved Algorithm For Computing Logarithms Over GF(p) and Its Cryptographic Significance"*, (pgs. 106-110); IEEE Transactions on Information Theory, Volume 24, Number 1, January 1978
pwk	C30	Pointcheval and Stern, *"Provably Secure Blind Signature Schemes"*, (pgs. 252-265); Advances in Cryptology, Proceedings of the ASIACRYPT '96, Kyongju, Korea, November 1996, Springer 1996
pwk	C31	Rivest, Shamir, and Adleman, *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,"* (pgs. 120-126); Communications of the ACM, Volume 21, Number 2, February 1978
pwk	C32	*"SKIPJACK and KEA Specifications"*, (pgs. 1-23); NIST, May 29, 1998, [online], [retrieved 2001-07-10], retrieved from the Internet, URL:http://csrc,nist.gov/encryption/skipjack-kea.htm
pwk	C33	Stadler, Piveteau, and Garnenisch, *"Fair Blind Signatures"*, (pgs. 209-219); Advances in Cryptology, Proceedings of the EUROCRYPT '95, International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21-25, 1995, Springer 1995
pwk	C34	von Solms and Naccache, *"On Blind Signatures and Perfect Crimes"*, (pgs. 581-583); Computers and Security, Volume 11, Number 6, 1992
pwk	C35	Wu, *"The Secure Remote Password Protocol"*, (pgs. 1-15); Proceedings of the 1998 Network and Distributed System Security Symposium, Internet Society, January 1998
pwk	C36	Zuccherato, *"Methods for Avoiding the 'Small Subgroup' Attacks on the Diffie- Hellman Key Agreement for S/MIME"*, (pgs. 1-11); IETF Internet-Draft (work in progress), June 1999, [online], [retrieved 2001-08-29], retrieved from the Internet URL:http://www.ietf.org/proceedings/99;ul/1-D/draft-ieft-smime-small-subgroup-ol.txt

EXAMINER Paula Klimach	DATE CONSIDERED 10 June 2004